Title:	*ENACT Roadmap*
Authors:	*Adrian Irala (Indra), Hui Song (SINTEF), Anne Gallon (Evidian), Nicolas Ferry (CNRS), Erkuden Rios (Tecnalia), Eider Iturbe (Tecnalia), Arnor Solberg (Tellu), Andreas Metzger (UDE), Stéphane Lavirotte (CNRS), Jean-Yves Tigli (CNRS), Vinh-Hoa LA (Montimage), Luong Nguyen (Montimage), Elena González-Vidal (Beawre), Victor Muntés-Mulero (Beawre)*
Editor:	*Adrian Irala (Indra)*
Reviewers:	*Erkuden Rios (Tecnalia), Arnor Solberg (Tellu)*
Identifier:	*Deliverable # D6.6*
Nature:	*Report*
Date:	*09 April 2021*
Status:	*Final*
Diss. level:	*Public*

Executive Summary

This deliverable presents the roadmap by the ENACT partners on the results after the end of the project, as well as research challenges that remain open toward achieving DevOps for IoT, which we hope may serve as inspiration to researchers, entrepreneurs and industrial stakeholders pursuing innovation in smart IoT systems (SIS).

The research leading to these results has received funding from the European Community's H2020 Programme under grant agreement n° 780351 (ENACT).

Members of the ENACT consortium:

SINTEF AS	Norway
EVIDIAN SA	France
INDRA Sistemas SA	Spain
Fundación Tecnalia Research & Innovation	Spain
TellU AS	Norway
Centre National de la Recherche Scientifique	France
Universitaet Duisburg-Essen	Germany
Istituto per Servizi di Ricovero e Assistenza agli Anziani	Italy
Baltic Open Solution Center	Latvia
Elektronikas un Datorzinatnu Instituts	Latvia
Montimage	France
Beawre Digital SL	Spain

Revision history

Date	Version	Author	Comments
20/03/21	V0.1	Adrian Irala (Indra)	First complete version
22/03/21	V0.2	Adrian Irala (Indra)	Second version incorporation first comments and feedback from the internal review
25/03/21	V0.6	Adrian Irala (Indra)	Final review to internal review. Revised by Erkuden Rios (Tecnalia)
09/04/21	V1.0	Adrián Irala (Indra)	Final version of the document

Contents

1 Introduction

This deliverable presents the roadmap for the ENACT partners and results after the end of the project as well as some challenges that remain open toward achieving DevOps for IoT, which we hope may serve as inspiration to researchers, entrepreneurs and industrial stakeholders pursuing innovation in Smart IoT Systems (SIS). The objective of this document is to prepare and summarize a set of follow-up activities to fully exploit the ENACT results and enable the partners delivering the identified project values to the targeted users after the project end.

The ENACT roadmap, presented in section 2, is organized along different dimensions: first, the four routes towards DevOps for IoT are presented (commercialization, community, technology transfer, and domains). Second, following the introduction to these routes, the individual exploitation plans identified by each partner of the project are presented. Finally, the section introduces the joint exploitation plans as a result of the collaborative efforts envisioned by the partners once the project ends.

Section 3 collects the main challenges solved for each tool during the project, as well as the open challenges that might be of interest to the community in order to continue with the work carried out in ENACT and further progress in SIS DevOps innovation.

2 The ENACT Roadmap

2.1 Four routes towards DevOps for IoT

The business roadmap of the ENACT project is based on an open-source strategy. The technical results of the project are a set of tools to enable the DevOps practice in the realm of smart IoT systems. Most of the ENACT tools, named enablers, are open-source solutions, and hosted in public GitLab repositories (https://gitlab.com/enact). The target users of these open-source tools are the DevOps teams of IoT applications, who may integrate some of these tools with other tools, including general-purpose DevOps tools and home-made tools particular to their products, to build their own DevOps environment. The business challenge for ENACT is how to lead its open-source tools to the potential users.

For the exploitation of the ENACT results and their sustainability, we define four different routes. These four routes are complementary to each other, and together form the business roadmap for ENACT. The ENACT partners have been following these routes to exploit the results and will keep following them after the project ends.

1. **Commercialization:** Providing commercial products and services based on the open-source tools.
2. **Community:** Building the community for external developers to participate in the further development of the ENACT projects, and facilitating potential users (DevOps teams) to select the open-source tools themselves and integrate them into their DevOps environments.
3. **Knowledge & Technology transfer:** Transferring the knowledge gained about DevOps for trustworthy smart IoT systems via lectures, courses and student supervision; continuing the research through subsequent projects, and helping third party organizations to wrap the open-source tools into commercial services.
4. **Domain solutions:** Building up ready-to-use DevOps environments for a particular domain, and exploiting the products that are developed under the DevOps environments.

We elaborate the four routes in the rest of this section, describing the relevant ENACT partners, the external services and the concrete plans. Figure 1 presents these four routes. Commercialization, community and knowledge and technology transfer routes are oriented towards DevOps teams for IoT

applications, while domain solutions are oriented towards customers and end-users in these domains. The partners following each of these routes are also indicated:

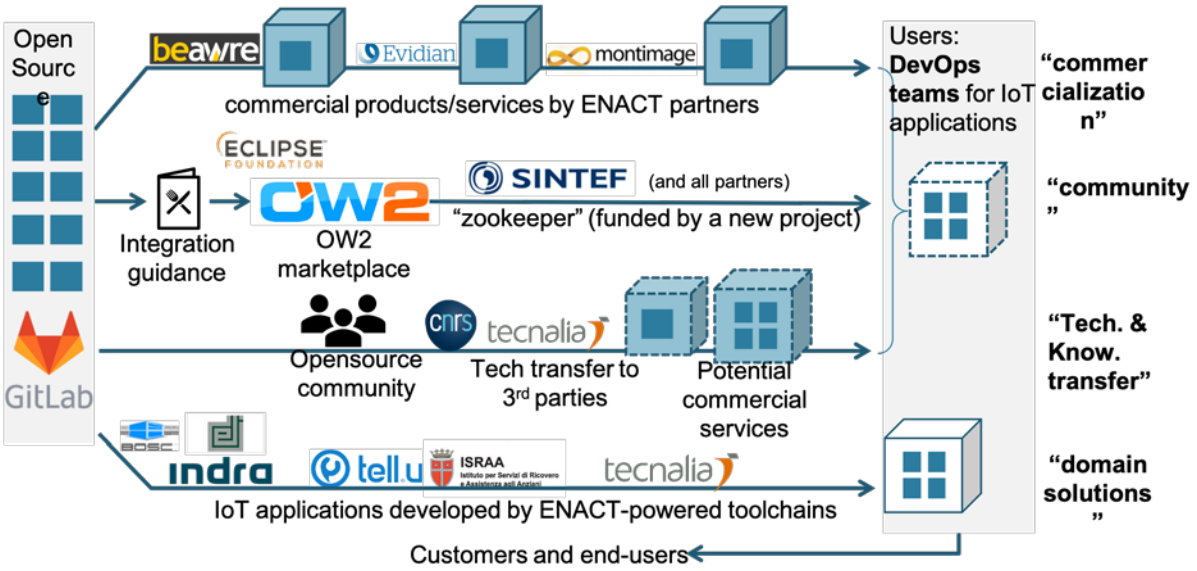

Figure 1: The four exploitation routes for the ENACT results

2.1.1 Commercialization

Three companies in the consortium, Beawre, Evidian and Montimage, are providing commercial products and services based on ENACT enablers.

Beawre is a start-up company founded during the ENACT project with the conviction that the idea promoted and the related solution developed in T2.1 has a large market potential. Its main product is the risk management tool. The business model of Beawre is based on open-source and SaaS. The core software is the open-source risk management tool, which is developed by Beawre and partially funded by the ENACT project. In particular, the code has been published as an Eclipse Research Project[1]. At the same time, they operate a set of software instances in the cloud, and provide the tool as a ready-to-use service to their customers. In addition, they also provide consultancy services to the customers on the risk management method and process, and evidence collection for regulation compliance. Currently, the customers include software DevOps teams and construction teams. The table below summarizes the main exploitation plan of Beawre:

Exploitation solution	A summary of the main achievements and exploitation related to Beawre both in terms of business level achievements and technical level exploitation is provided in this table. Beawre was created in January 2019 and since then it has been able to validate the need for continuous risk management and the solution of the company, partially developed in this project. In terms of validation, there are several clear indicators that serve as a proof: • On July 21st, 2019 we **signed a first contract** with the following consortia: Vinci Construction Grands Projets S.A.S. (France), Ferrovial Agroman SA (Spain), Razel-Bec S.A.S. (France), Dodin Campenon Bernard S.A.S. (France), Campenon Bernard Sud-Est S.A.S. (France), GTM Sud S.A.S. (France), and Chantiers Modernes Sud S.A.S. (France). This consortium works under a contract with

[1] https://github.com/eclipse-researchlabs/enact-rm-API

Fusion for Energy (F4E), the European Union's organization for Europe's contribution to the International Thermonuclear Experimental Reactor (ITER), to build the Tokamak complex and to design and build several auxiliary buildings at Cadarache, north of Aix-en-Provence in southern France. The ITER project is a first-of-a-kind global collaboration in the field of energy. It is the world's largest experimental fusion facility and is designed to demonstrate the scientific and technological feasibility of fusion power. Because of the characteristics of this unique construction project and the criticality of the infrastructure, quality and risk control is essential. The technology developed in ENACT is used as the core of the solution we deployed for this consortium to implement continuous risk control processes. Our current agreement allows companies to use our solution for 3 years.

- **Beawre among the 10 winners of the CEMEX Startup Competition 2020**: Almost 700 construction revolutionaries competed to become the missing piece in the industry during the fourth edition of CEMEX Ventures Construction Startup Competition, the most powerful startup challenge in the construction industry. After reviewing hundreds of applications, Construction Startup Competition selected 10 winners, and Beawre was one of these 10 winners, presenting their solution for continuous risk management. This competition has been the prime event of CEMEX Ventures since its beginnings. The first edition was celebrated in 2017 and it has kept getting bigger and more relevant within the ecosystem year after year. Beawre was afterwards invited to participate in a Digital Pitchday, where we pitched to top Management representatives from CEMEX Ventures, Ferrovial, Hilti, VINCI Group's Leonard and NOVA by Saint-Gobain on December 2nd. In addition, the audience of this digital session was composed of experts from the construction and investment industry under the framework of the Builtworlds Venture Conference event. With this new achievement, Beawre confirmed the growing need for the construction industry to control risks continuously and in real time. Through EU H2020 projects ENACT and PDP4E, Beawre has developed part of their core technology, allowing us to get our first pilots with large construction projects and further visibility and credibility in front of a global audience. Figure 2 shows part of the video published by CEMEX Ventures to announce the winners[2].
- **Beawre selected in the Top 50 ConTech Startups of 2020**: Beawre has been selected to be part of the CEMEX Ventures TOP50 ConTech Startups list, which includes the 50 most promising new solutions from the 2020 construction ecosystem and the cities of the future. Beawre has been selected as a top startup to help the construction sector to improve project productivity, through their solution for continuous risk management. CEMEX Ventures selects the TOP50 ConTech Startups with the projects it receives in its annual challenge for entrepreneurs in the industry, Construction Startup Competition, added to the flow of new solutions that it shares with its strategic network of investors and companies working in innovation and investment in construction, as well as with the

[2] Meet The Winners: Construction Startup Competition 2020 | CEMEX Ventures: https://www.cemexventures.com/winners_constructionstartupcompetition2020/

	collection of multiple startups that contact them directly through events, social networks or its website. The 2019 list has numerous solutions that, during 2020, obtained relevant investment rounds, bringing this industry closer to a more technological, digitized, and less fragmented environment. • **Beawre selected finalist in the AppChallenge 2020 of Singapore Airlines**: Beawre was selected by Singapore Airlines among several hundreds of companies as one of the top 10 most promising solutions for aviation in 2020, presenting an IoT-based solution for continuous risk management related to ground equipment control at Changi airport. **Beawre selected by the Dealflow.eu H2020-funded initiative as one of the "Raising Stars" in the EU**: Beawre was selected by the Dealflow.eu project consortium as one of the "Raising Stars" in the EU in October 2020, as shown in Figure 3. Through this recognition we signed a partnership with Deloitte, HI Capital and Dealroom.co to increase our traction and access to investment.These awards have generated a significant presence for Beawre in digital media worldwide. To see some examples, please refer to Appendix A.
Type of IPR	Dual license: Open Source (through Eclipse Foundation) / Proprietary Software (as SaaS).
Roadmap	Beawre has already developed a commercial version of their product based on the technology developed in ENACT and also in the H2020 PDP4E project. In particular, we are leveraging the research, innovation and development of technology for continuous risk management developed in the ENACT Risk Management enabler. Specifically, this first solution includes technology for asset management, the first version of our risk management engine and a dashboard system. We have also embedded part of the technology developed in ENACT for evidence collection. Our immediate plans to commercialize Beawre's solution include: • Closing an agreement with an airline to commercialize Beawre's solution: we are already at the negotiation stage. We are currently looping through reviews with legal experts of the agreement to deploy a pilot of our risk management solution during 2021 and offering them SaaS from the beginning of 2022. This solution will include the technology developed in ENACT for asset management and dashboarding mechanisms. The solution leverage data from IoT devices attached to the ground equipment at the airport or devices carried by the airport operators. • Closing an agreement with one of the largest construction companies in the world to start using our risk management solution in a project in the UK: we currently have the confirmation that our solution will be used in a construction project, immediately. This solution includes technology for asset management, the first version of our risk management engine and a dashboard system, developed in ENACT. • Closing an agreement with a large construction company to start using our evidence collection and asset management technology: our potential customer has already confirmed that they plan to start using

	our technology in an ongoing construction project in Spain, as soon as practical. This solution includes technology for evidence collection and asset management, developed in ENACT. • We also plan to further explore the use of the Risk Management enabler to evaluate its capability to support TellU's risk analysis and risk management procedures related to their services, and to facilitate the reporting for ISO 27001 compliance.

Table 1. Beawre exploitation plans

Figure 2: CEMEX Ventures video to announce the winners of the Construction Startup Competition 2020.

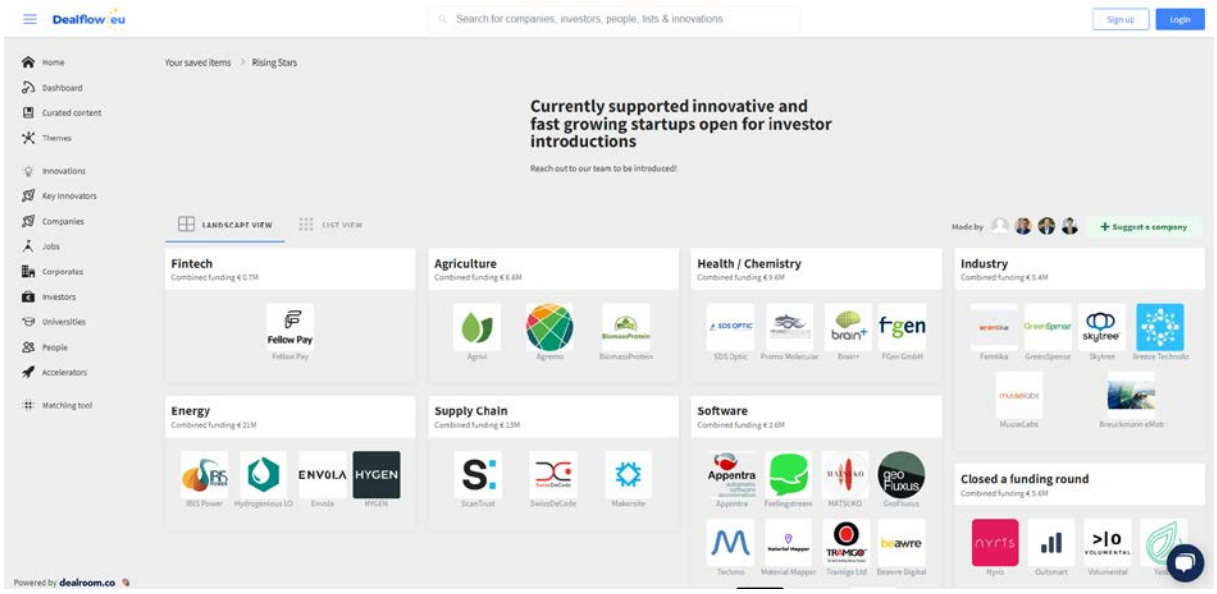

Figure 3: Beawre detected as one of the "Raising Stars" in the EU by the H2020 Dealflow.eu project.

Evidian developed the Context-Aware Access Control (CAAC) enabler during the ENACT project and will integrate it in the Evidian standard offer as a key component of the new "Prescriptive IAM" offer. The new CAAC component will be their answer to the requirement of effective and flexible access

control on IoT devices, under the background of the convergence between IT (Information Technology) and OT (Operation Technology).

Exploitation solution	Software tool: Context-aware access control and authorization mechanisms for smart IoT systems. The Context-Aware Access Control tool is an evolution of the authentication and authorization mechanisms provided by Evidian Web Access Manager (WAM) intended for the Internet of Things. It will be integrated in the Evidian standard offer as a key component of the new "Prescriptive IAM" offer.
Type of IPR	Proprietary Software
Roadmap	During the course of ENACT, Evidian has taken the Step 1 in the company Product Life Cycle Management process, which leads to a formal decision to include the CAAC in the Evidian IAM official roadmap. Starting from the end of ENACT, Evidian will launch the Step 2 of the Product Life Cycle Management, whose goal is to obtain a GO for industrialization and announcement of the new solution component. TRL 6/7 is reached at the end of the project. TRL8/9 is expected 2 years later. From the GO for industrialization and announcement, the Product management team will prepare sales and training material, the Delivery team will prepare software distribution, and the Support team will prepare helpdesk processes.
	Two years after the end of ENACT, Evidian will launch the Step 3 of the Product Life Cycle Management, whose goal is to obtain a GO for General Shipment. Press release and communications about the new product offer will be then prepared, and the new solution can then be offered for sale.
	Evidian will first target the sector of HealthCare, considering the success that resulted from the Digital Health use case in ENACT. Then, other Evidian customers will be addressed, as well as new prospects in each domain addressed by Evidian: Manufacturing/Retail/Transports, Public Health, Finance/Services and Telecom/Media/Utilities. The objective is to deploy the solution five years later at key customers. At the same time, Evidian aims to be recognized by analysts as a major European vendor for IoT security.

Table 2. Evidian exploitation plans

The core business of Montimage is developing tools for testing and monitoring networks, applications and services; in particular, for the verification of their functional, performance (QoS/QoE) and security aspects; and, for improving context awareness and end-user trust. Montimage developed the Test and Simulation (TaS) enabler and the Root Cause Analysis (RCA) enabler within ENACT based on their expertise in the test and monitoring domains, and will keep improving the capabilities of the two enablers in terms of functionalities and genericity in order to enhance their technology readiness and market maturity levels. The two tools have reached today the technical readiness level TRL 5 and more technical effort is planned in the next year to be able to start their commercialization. Montimage plans to include the TaS and RCA enablers as part of their portfolio starting from mid-2022. A dual exploitation is planned: a light version of each enabler will be available as an open-source solution for researchers and academic institutions and a complete version will be commercially exploited as licenced software.

Exploitation solution	The Test and Simulation enabler (TaS) has been developed in the context of ENACT project. It allows to create a digital twin of an IoT environments in order to simulate and test different functional, performance, scalability and security scenarios. The TaS enabler will be improved in the context of a new H2020 project called PRECINT that will start in September 2021. More effort to industrialize the tool is needed to apply it to different cases and assess its functionalities to fit the market needs. A light version of the enabler is proposed today as an open-source solution. A more complete version will be proposed as a SaaS solution by mid-2022.
Type of IPR	Test and Simulation: Dual licence (MIT open-source solution and a commercial one with more features)
Roadmap	Test and Simulation enabler: TRL 8 at the end of the project. The TaS enabler code will be assessed to prepare its commercialisation. More functionalities will be provided to facilitate the exploitation of the evaluation results by providing general or concrete recommendations to mitigate a detected error/risk. TaS will also be evaluated in the context of other case studies to validate its genericity. The PRECINT project will provide several of these contexts. TaS will be added to the Montimage portfolio starting from mid-2022. It will be exploited by selling licences and by offering IT services around it to adapt to specific customers' needs.

Exploitation solution	The root cause analysis (RCA) enabler has been developed in the context of ENACT project. This tool is complementary to the MMT monitoring suite already exploited by Montimage and will be integrated in this monitoring ecosystem to provide a better insight on the origin of detected errors and attacks and help administrators/operators to select the best remediation strategy and automate the reactions. The RCA tool will be improved and extended in the context of other running H2020 projects (INSPIRE-5GPlus, SANCUS, VeriDevOps). In addition, it will play a very important role in Montimage's commercialization strategy. It will be proposed as a standalone licenced solution and will also be integrated within the MMT monitoring suite of Montimage as a paid extension.
Type of IPR	Root Cause Analysis - Dual licence: Community version (MIT open-source + free) and Pro version (with more features).
Roadmap	Root Cause Analysis: At the end of the project the RCA enabler has reached the technology readiness level of TRL5 - technology validated in relevant environment. It will be fully exploited by mid-2022..

	Montimage will continue the development work of RCA tool to adapt it to different contexts (5G networks, Industry4.0 environments, etc.) by taking advantage of running H2020 projects (notably, INSPIRE-5Gplus). Montimage will then incorporate the research and technical outcomes related to root cause analysis into its MMT monitoring framework product that will extend its capabilities with unique technical and market innovations. In this way, the users will obtain better insight on detected functional and non-functional incidents. The integrated module will be called MMT-RCA and will start to be commercially exploited by mid-2022 by selling licences and offering IT services around it to adapt to specific customers' needs.

Table 3. Montimage exploitation plans

All the three companies use their marketing channels to promote the products. Due to the connection among ENACT enablers, this will also lead to the exposure of other enablers and the ENACT framework among the customers of these companies.

2.1.2 Community

The objective of the community-based promotion is to increase the exposure of the ENACT framework and the individual tools, as well as creating communities around them. By making promotion of the open-source tools, opportunities are opened to sell services around them and also other related commercial products or services, and it facilitates DevOps teams in the integration of the ENACT open-source enablers into their DevOps environments. A good example of community building achieved in the project is the SMOOL community, which successfully integrates various of the solutions developed in ENACT, and even some are made available as part of SMOOL (e.g., the Security-aware SMOOL IoT Platform - Control Enabler).

The main vehicle we will use for this objective is the OW2 open-source project[3] for the ENACT DevOps Framework. OW2 is an open-source consortium based in Europe dedicated to fostering open-source projects. OW2 provides services and events to control the quality of open-source projects, promote the community involvement of projects, and support the further exploitation. ENACT has applied to be an OW2 project in early 2020, and after several rounds of improvement together with the OW2 members, was finally accepted in early 2021, and listed in the OW2 marketplace. The plan is to add and register the ENACT tools one after the other. GeneSIS is already approved, and the next tool planned to be added is DivEnact. We expect the process to be smooth as for GeneSIS as the rules defined in WP5 for the development and maintenance of the tools (e.g., repositories, structure of the repositories, documentation, etc) are the ones typically adopted for open source solutions.

The OW2 project for ENACT will serve as the main entrance for potential users to understand the ENACT DevOps Framework and to select the ENACT tools they are interested in. To facilitate the users in getting started, we provide a set of guidelines, including the decision table for selecting ENACT tools, the relation and compatibility with external IoT tools and platforms, etc., as documented in Deliverable 5.4. SINTEF will remain the "zookeeper" after the project ends, for users to consult about how to use the framework, and also to promote project. These activities will be funded by two follow-up projects in which SINTEF is involved, where its main outcomes from ENACT: the GeneSIS and DivEnact tools, will be further developed, until 2024.

[3] https://projects.ow2.org/view/enact/

Exploitation solution	In addition to their own enablers (DivEnact and GeneSIS), SINTEF is in charge of maintaining the whole "ENACT framework", as the main contact point for potential users, and provides essential consultancy support for users to get start with ENACT tools.
Type IPR	Open Source
Roadmap	During the ENACT period, SINTEF has gone through the procedure with OW2 to create the open source project to cover the ENACT framework. The project is now accepted and listed in the OW2 marketplace. As a first step, we have released the GeneSIS tool as the sole component of the open source project. We are now in the process of adding other tools into the project gradually. Within at least four years after ENACT ends, SINTEF will serve as the project manager for the ENACT project in OW2, maintain the user guiding materials, forward technical questions and issues to relevant partners, and promote the ENACT approach and tools as a whole in conferences and other venues. These activities will be funded by subsequent projects (e.g., FLEET NRC project) in which SINTEF continues in developing the ENACT results.

Table 4. SINTEF exploitation plans: Community for the entire framework

2.1.3 Technology & Knowledge Transfer

ENACT partners are also seeking for opportunities of technology transfer, for third-parties to exploit the open source tools as products or services. For this purpose, we prioritize permissive licence, such as Apache 2.0, for ENACT enablers, so that we do not set up limitation for commercial usages of the tools.

In this direction, CNRS as the provider of the ACM and BDA enablers is in touch with SATT (Technology transfer acceleration company) associated University Côte d'Azur, and they have started the initial steps to prepare for the IPR protection.

TECNALIA is currently under negotiations of commercialization potential of the Security Monitoring Enabler with a major vendor of Security Operation Center (SOC) services in Spain. In all cases, TECNALIA would keep the R&D license over the Enabler.

Exploitation solution	Software tool for continuous development, orchestration and deployment of software across IoT, Edge, and cloud infrastructure, supporting the diversity-oriented deployment of software on large fleets of IoT-edge-cloud resources.
Type IPR	Open Source
Roadmap	During the project period, SINTEF is focused on scientific dissemination of the ENACT tools. Within 4 years after ENACT ends, SINTEF will concentrate on further developing the ENACT results through subsequent research and innovation projects. SINTEF has already secured two projects for this purpose: The first one is an innovation project funded by the research council of Norway with Tellu and another Norwegian SME, focusing on

	consolidating the fleet deployment concept and tools and apply it to companies' development environment. The second project is an H2020 Research and Innovation Action, where SINTEF will work on the use of fleet deployment for distributed trust management among IoT devices. Towards the end of the innovation project (scheduled at 2024), SINTEF foresees the use of the deployment tools by two companies in their everyday DevOps environment, which means a TRL at 8. In addition, SINTEF will utilize the innovation project to prepare for the technology transfer.

Table 5. SINTEF exploitation plan: Automatic deployment tools

Exploitation solution	Software tool: A security monitoring tool that offers IoT system operators the capability to control the security status of their system with a minimal intervention and full integration with security-by-design mechanisms used, following the DevOps approach. The prototype includes heterogeneous monitoring agents that are distributed in the IoT system architecture to capture network, application and device layer data. The tool performs signature-based intrusion detection and Artificial Intelligence-based anomaly detection and cyber incidents and attack detection. The tool is composed of both monitoring agents and back-end. The services in the backend could be offered as SaaS, provided the open-source licences of the baseline tools allow it.
Type of IPR	Dual License. The tool integrates open source software pieces with proprietary pieces, and two versions are expected: Community version (open-source + free) and Pro version (with advanced monitoring and detection features).
Roadmap	TRL5 in the project and TRL7 1 year after.

Table 6. Tecnalia exploitation plan: Security monitoring

Exploitation solution	Open source tool: A Security-aware ontology-based IoT middleware based on SMOOL (SOFIA open source). The software is composed of the server and the clients that publish and consume data in IoT environments. The ENACT enhancements have enabled the transmission of security metadata captured in SMOOL ontology as security concepts. Thus, the SMOOL middleware is now secure and facilitates establishing security metadata monitoring as well as ensuring secure communications and security policies' enforcement, according to the IoT environment needs in each case. The solution is fully integrated with ThingML and GeneSIS modelling solutions.
Type of IPR	Open source.
Roadmap	TRL5 in the project and TRL6 1 year after. The SMOOL IoT platform has quite a long history since SOFIA project ended, and it has its own community and well-known bitbucket

	placeholder. Therefore, it is most likely to remain as such, and only the reference integrated in the ENACT framework in OW2 ecosystem.

Table 7. Tecnalia exploitation plan: Security-enhanced SMOOL SOFIA

The knowledge gained during the project will be transferred, via subsequent projects bilateral or research, lectures/courses/ supervision, consultancy. UDE will continue exploiting the ENACT results, tools and technologies by transferring the knowledge obtained during the project into a prototype software solution. The expected roadmap for the first knowledge transfer is expected a TRL4 right after the end of the project.

Exploitation solution	The main exploitable solution developed by UDE in ENACT is the Online Learning Enabler – OLE. The OLE is an enhanced reinforcement learning module taking into account the structure of the IoT systems' adaptation space, and offering the following main advantages from the state of the art: *a) Capturing large continuous state and adaptation spaces:* Existing OLE approaches for self-adaptive information systems exhibit an important shortcoming that limits the degree of automation that may be achieved. Most existing approaches use a lookup table to represent the learned knowledge, which requires information system engineers to manually quantize environment states to facilitate scalability if the environment has a high number of states. Such manual activity may be expensive and potentially unreliable and may require information not available at design time due to design time uncertainty. Furthermore, such table-based approaches cannot cope with adaptation action represented by continuous variables as they might occur when adapting a system through self-parametrization. OLE automates the aforementioned manual activity by employing policy-based RL as a fundamentally different type of RL. In simple terms, policy-based RL represents the learned knowledge as an artificial neural network. Our approach conceptually, formally and technically integrates policy-based RL into a well-known self-adaptive system reference model. Our approach thereby facilitates online RL for self-adaptive Smart IoT Systems without having to manually quantize environment states. Furthermore, our approach is able of handling adaptation actions represented by continuous variables. *b) Capturing large discrete adaptation spaces and system evolution:* Existing online RL solutions for self-adaptive systems propose randomly selecting adaptation actions for exploration during learning. The effectiveness of exploration therefore directly depends on the size of the adaptation space, because each adaptation action has an equal chance of being selected. In the presence of large, discrete adaptation space, random exploration thus may lead to slow learning at runtime. Further, existing online RL solutions are unaware of system evolution. They do not consider that a self-adaptive system, like any software system, may undergo evolution (typically during the DEV part of the DevOps loop). System evolution means that the adaptation space may change, e.g., existing adaptation actions may be removed or new adaptation actions

	may be added. Existing OLE approaches cannot cope with changes of the adaptation space. Existing solutions thus explore new adaptation actions only with low probability, and thus may take quite long until new adaptation actions have been explored. Our main contribution is to introduce exploration strategies for OLE that use feature models to give structure to the system's adaptation space and thereby leverage additional information to guide exploration. A feature model is a tree or a directed acyclic graph of features, organized hierarchically. An adaptation action is represented by a valid feature combination specifying the target run-time configuration of the system. By leveraging the structure of the feature model, our strategies guide the exploration process. In addition, our strategies detect added and removed adaptation actions by analysing the differences between the feature models due to evolution. Adaptation actions removed as a result of evolution are no longer explored, while added adaptation actions are explored first. *c) Explaining the adaptions generated by reinforcement learning:* To facilitate the observation and quality assurance of the OLE behaviour at runtime, T3.1 explored the use of explainable AI techniques. Reward decomposition is an approach in which several RL agents are trained in parallel on different aspects of an environment. At each time step the knowledge of the agents is aggregated to provide a global decision. To apply this method, it is necessary that the reward function of the examined environment can be decomposed into independent subfunctions. As a result, instead of returning a scalar value at each time step, the reward function returns a vector where each component reflects the reward of one subfunction or zero if there was no reward or punishment at the associated time step. For each component of the reward vector an independent subagent is trained, which receives the global state as observation and as reward only one component of the reward vector. To derive the action of the overall agent, at each time step the action values of all subagents are summed up.
Type IPR	Prototype software (available as open source research demo), TRL 4
Roadmap	The OLE has reached the expected TRL4 at the end of the project. As part of the exploitation roadmap for UDE, the following actions are ongoing at the time of reporting: • The concepts and prototypes underlying the OLE tool serve as basis for further development in the H2020 project DataPorts (RIA). Where, in particular, policy-based RL is leveraged to facilitate the proactive adaptation of data-driven business processes. DataPorts designs, implements and operates a cognitive ports data platform that: i) connects to the different digital infrastructures currently existing in digitized seaports, enabling the interconnection of a wide variety of systems into an integrated ecosystem, ii) sets the policies for trusted and reliable data sharing and trading based on data owners' rules and offering a clear value proposition, and iii) leverages on the data collected to provide advanced data analytics services based on which the

	different actors in the port value chain can develop novel AI and cognitive applications. To further mature the OLE solutions, UDE is currently working on a project proposal towards the HORIZON-CL5-2021-D6-01-09 call on "Climate resilient and environmentally sustainable transport infrastructure, with a focus on inland waterways". As this will be an IA, the ambition is to increase the maturity of OLE from TRL 4 (at the end of ENACT) to TRL 6-7.

Table 8. UDE exploitation plan

The knowledge gained during the project is already being transferred via lectures/courses as detailed in D6.5. This knowledge transfer to engineer and master students has already been implemented in a course run in 2020-2021 ("Middleware for Internet of Things"). To complete the training offer, a new course will be created next year: "Full Stack Software Engineering for IoT" for engineer and master students. In addition, CNRS will continue exploiting the ENACT results, tools and technologies by transferring the knowledge and technology obtained during the project with the support of SATT (Technology Transfer Acceleration Company). The expected roadmap for the first knowledge transfer is expected a TRL4-5 right after the end of the project (thanks to the smart-home use-case development).

Exploitation solution	Software tools for Actuation Conflict Management (ACM) and Behavioural Drift Analysis (BDA) for IoT systems.
Type of IPR	Dual License. The tools integrate open source software pieces with proprietary pieces, and two versions are expected: Community version (open-source + free) and Pro version (with advanced features).
Roadmap	During the project period, CNRS focused on scientific dissemination and also developing experimental prototypes to test the results of the ENACT tools on real cases (development of a smart home use case). CNRS already started discussions with the Technology Transfer Acceleration Company (SATT). If the maturation process is successful, the objective is to transfer the ACM and BDA technologies to a company to be determined through collaboration with the SATT. To achieve this objective, the ambition is to increase the TRL of ACM and BDA from TRL 4-5 (at the end of ENACT project) to TRL 6-7 two years after the end of the project (SATT "maturation process"). The final objective is licensing with an industrial partner with the help of SATT. In parallel, we are exploring the possibility of submitting new project proposals for BDA and already started discussions with partners (Fondation Université Côte d'Azur and industrial partners, as EDF R&D group, EpicNpoc (SME), GreenCom (SME), …

Table 9. CNRS exploitation plans

2.1.4 Domains

The three use case providers have all implemented their prototype DevOps environments, using the ENACT enablers together with external tools, and will gradually migrate the environment to their production environment. The exploitation plan of these partners will be mainly focused on the products that is being developed by the ENACT tools, rather than the tools themselves.

Exploitation solution	Indra has been focused on two different systems as part of the Rail Use case, the proposed use case for railways has improved the Indra solutions making use of the ENACT enablers to enhance the DevOps cycle of new innovative systems – aligned other innovation programs (Shitf2Rail and ECSEL) - exploiting and evaluating their potential. The selected innovative systems have been analysed, implemented and tested and are ready for exploitation: • **On Board WTI (Wireless Train Integrity):** This functionality is in charge of measure in real time train composition parameters to evaluate and report train consists. The on-board system, based on WSN Sensors among the composition, provides the necessary information to determine the rolling stock material that composes the consists and evaluates and ensures through an on-board unit, the integrity of it showing the driver the integrity status but integrated with the TMS through a centralized cloud service. • **Logistic and Maintenance System:** This functionality provides information to register, locate both rolling stock material and On-Track signalling devices and inform about their status. This functionality is required to solve the rail environment needs to locate and monitor the status of the big heterogeneity and flexibility of the compositions and signalling devices, making a special emphasis on the freight compositions, to optimize the rail business operation. The points that are optimized into the rail framework are the management of the rolling stock, cargo tracking, etc. To this end, it is required deploying IoT On Track, On Board, and Cloud solutions to track and manage the rolling stock material data and to perform predictive maintenance. During the project, the systems have been improved making use of different DevOps enablers: - **Security and Monitoring** (S&P): In charge of monitor and actuate over the On Board infrastructure to guarantee its Safety and Security characteristics. - **Automated Deployment**: To monitor performs software remote deployments on the rail equipment to keep all the devices with the desired software version. - **Behaviour Drift Monitoring**: To monitor the behaviour of the equipment to detect deviations related with the proper defined behaviour for them. - **Actuation Conflict Management**: To detect conflicts that may appear in the Use Case operation and create a protocol to prioritize the conflict actions. - **Testing and Simulation too**l: To simulate a part of the Use Case infrastructure and make a Digital twin of it to be evaluated.

	- **Root Cause Analysis** (RCA): To detect possible failures that may occur in the Use Case infrastructure informing about the most likely cause for that fail. The results of ENACT have improved the Rail systems of Indra for future exploitation not only focused on the presented systems, but on an IoT Platform for Rail able to manage Agile deployments (Cloud and On-Board components to provide an automation mechanism to deploy new releases on field), monitoring of all the components of the different systems and to provide extra capabilities for security and conflict management to robust the offering of new rail services.
Type of IPR	Proprietary Software
Roadmap	The presented solutions as well as the IoT Platform for Rail and other related solutions that will be use of this new features are planned to be commercialized during the next 3 years (due to the different maturity of the products that make use of this technology)

Table 10. Indra exploitation plan for ITS domain

Exploitation solution	A summary of the main achievements and exploitation related to TellU and the Digital Health use case both in terms of business level achievements and technical level exploitation is provided in this table: - The use case itself has evolved from being a prototype development in the beginning of the project to being a production ready system recently sold to customers and already deployed for remote supervision of several hundred patients suffering from chronical diseases such as COPD, Kidney and Diabetes. Moreover, it has been applied for remote supervision and following up of Corona patients in several municipalities in Norway. The application has got attention from the World Health Organisation (WHO) and will be presented at a WHO conference this spring by one of our customers (a Norwegian municipality). This again leads to attention from Norwegian media houses putting this on their news (including TV news). The support and exploration we have been able to do in ENACT in particular related to efficient DevOps processes, Security and trustworthiness aspects and exploring the ENACT enablers and tools have been significant to reach this success. In particular, the Personal Health Gateway, which is a core component managing the IoT and edge part of our service, the ENACT project has been significant for its evolution. Furthermore, the outcome of the ENACT project will be further explored to ensure a scalable and trustworthy service as we see both the potential and the need to further improve our DevOps process to cope with the scale of distribution we foresee. Thus, we have already initiated some following up projects and activities to further evolve on results from the ENACT project. In particular the deployment and orchestration enabler bundle where we have successfully applied for a following

	up R&D project that is receiving funding from the Norwegian Research Council - During ENACT TellU has experienced significant growth, both related to exploiting the ENACT use case to build a production ready remote patient monitoring service and by evolving its already existing remote supervision services in the welfare domain (camera-based and sensor based supervision), which evolution has also been explored as part of ENACT. In figures TellU has grown its revenue 10 times during the ENACT project period (from 0.7 M€ in 2017 to 7 M€ in 2020) and has grown from 5 employees in 2017 to about 40 to date. - In particular TellU wants to explore ENACT results to enable to further scale our largely distributed IoT based services. In particular for the Personal Health Gateway we will explore ENACT results. Moreover, existing digital health services such as Remote Patient Monitoring and Digital Supervision will be evolved and improved applying gained knowledge and results from the ENACT project
Roadmap	- TellU has or are investigating to exploit several of the ENACT enablers. In particular: o TellU is already exploiting the part of the ENACT Orchestration and Continuous Deployment Enabler in its DevOps process in particular, the support for the efficient development and management of code deployed on edge and IoT devices related to the ThingML tool. Moreover, the ENACT GeneSIS tool is explored to support the continuous deployment on the edge and IoT level. o We have started to exploit the DivEnact framework (which is part of the ENACT orchestration and continuous deployment bundle) that supports the management of large number of largely distributed but similar edge and IoT deployments. TellU foresees to evolve our exploitation of DivEnact further to be able to better manage our large-scale deployments of services we deploy in people's homes related to our Telecare services. These services need to be efficiently and securely managed across the IoT, edge and cloud space. This is planned and prepared and is also further funded by a new innovation project supported by the Norwegian Research Council. o The Context Aware Access Control (CAAC) tool, which is part of the ENACT Security and Privacy Monitoring and Control Enabler is prepared to be further explored. In particular since this provides interesting opportunities in terms of providing access to IoT and edge devices such as surveillance cameras related to various context. For example, in case of a fire alarm it may be an opportunity to provide access to the firefighters, while in the normal state the access is purely granted to authorised health personnel. o We also plan to further explore the Risk Driven Decision Support enabler to evaluate its capability to support our risk analysis and risk management procedures related to our

	services, and to facilitate the reporting for ISO 27001 compliance.
	As the Expected TRL is around 5 for most of the enablers at the end of the project. Full exploitation is expected 3 years after the project end.

Table 11. Tellu exploitation plans for eHealth domain

Exploitation solution	Tecnalia has developed IoT applications for energy efficiency and user comfort for Smart Buildings in its singular Kubik infrastructure. The exploitation solution of ENACT products for Tecnalia will be mainly through the use of Kubik as a testbed for the IoT domain and the development of software intended to the energy management in buildings. The IoT applications for Smart Buildings will benefit from the following DevOps Enablers developed in the project: - **Actuation Conflict Management (ACM)**: To resolve actuation conflicts when two or more different IoT applications try to send simultaneously conflicting orders to the same actuator or when different actuators act on the same physical variable in a contradictory way. - **Behavioural Drift Analysis (BDA)**: To monitor behavioural drift or unexpected behaviour of and IoT application when controlling a smart environment for ensuring that the SIS operates as expected at run-time and help identifying the symptoms of a drift. - **Security and Privacy Monitoring and Control using the SMOOL IoT platform**: To actively monitor the network traffic to identify whether the traffic deviates from normal behaviour, malicious actors or unauthorised entities try to access resources without permissions. In addition, to generate secure actuation through the SMOOL IoT middleware by using authentication tokens that identify the authorised applications and allow the use of security policies in sending orders to actuators. - **Online Learning and Self-Adaptation Enabler**: To train a Reinforcement Learning (RL) based agent to make a direct control of the HVAC, thermostat or other climate control system, device system of a building, improving comfort and reducing energy consumption. This Enabler allows to quickly create and automatically adapt energy efficiency strategies to different buildings and climate control systems. - **GeneSIS**: For continuous deployment of IoT applications. GeneSIS is also integrated with SMOOL and ThingML models. GeneSIS will be used in the automatic deployment of secure IoT applications that allow MDE to ease the design, configuration and deployment of security mechanisms used at runtime.

	Tecnalia will offer services to customers for developing and testing IoT applications for Smart Buildings, mainly related to efficient energy management without compromising the user comfort. These IoT applications will ensure the security and privacy of communications, the robustness of the IoT control, prevent any concurrent access to actuators or conflicts on actions over controlled physical variables, reduce behavioural drift, and acquire self-adaptation strategies to control the environment. The solutions provided by Tecnalia in the Kubik building will be the facility to run and test IoT applications, a secure and private environment, built-in security strategies in the software, and the ability to run several applications in parallel sharing sensors and actuators.
Type of IPR	Proprietary Software as SaaS
Roadmap	The full exploitation of Kubik as an infrastructure to develop and test energy efficiency and user comfort trustworthy IoT applications for Smart Buildings is expected to happen in 3 years after project completion due to the maturity of the ENACT Enablers. In parallel, Tecnalia is committed to disseminate ENACT benefits for Smart buildings in workshops, conferences and magazines of the domain, just as we are currently disseminating ENACT in Casadomo (https://www.casadomo.com/) online magazine by Grupo Tecma Redes, the leading Spanish publisher in information and knowledge generation on Energy, Sustainability and New Technologies in Buildings and Cities.

Table 12. Tecnalia exploitation plan for smart buildings

2.2 Joint exploitation plans

ENACT project partners have also identified joint exploitation assets as a result of the combination of different solutions and technologies obtained in the project. These assets that collaboratively shall be exploited offer a unique added value that cannot be acquired through the individual exploitation of these assets, and they provide a great example of how the different tools can work together to unlock new potential in the DevOps ecosystem.

The joint exploitation plans are presented below. In these plans, each joint exploitation asset is described, together with its potential users, the exploitation mechanism, IP protection and Roadmap. Finally, the added value of the joint asset from a DevOps and Trustworthiness perspective is presented at the end of each table:

2.2.1 Continuous Deployment with Actuation Conflict Management

Partners	SINTEF & CNRS	Tools	GeneSIS and Actuation Conflict Management
Name			Further Research

	Continuous Deployment with Actuation Conflict Management	Exploitation mechanism after ENACT	Technology transfer
Users/ Market	Users: DevOps engineers working on the software part of IoT systems with a focus on developers. Focus on systems involving actuators. Market: DevOps tool for IoT, in particular tools for deployment. Management of actuators	Roadmap	TRL at the end of the Project is expected to be 6. Exploitation plan: • Knowledge transfer via Project – Already in contact with EDF. • Sustainability via Project. Relation SINTEF – CNRS (string relationships with former employees from SINTEF in CNRS) • Knowledge transfer via courses. • Workshop CNRS – SINTEF are already planned.
Description of solution	There is currently no solution for managing actuation conflicts in a DevOps fashion. This is mainly due to the lack of integration with solutions for the continuous deployment of IoT systems. Our solution supports the deployment and orchestration of IoT systems over IoT, Edge, and Cloud resource, and the automatic identification of actuation conflicts and their resolution by DevOps teams	IP Protection	Open Source. Each partner maintains its own tool and related IPR
DevOps perspective	Continuous (in a DevOps fashion) management of actuation conflicts enabled by support the continuous deployment of systems over IoT, Edge, and Cloud.		
Trustworthiness perspective	Improve reliability and safety via **continuous** management of actuation conflicts. As well as reliability, resilience and availability via continuous deployment (via blue/Green deployment for instance)		

Table 13. Continuous Deployment with Actuation Conflict Management

2.2.2 Remote patient monitoring and assistant solution for smart co-housing

Partners	SINTEF, Evidian, ISRAA, Tellu	Tools	GeneSIS, DivEnact, Context-aware access control (CAAC)
Name	Remote patient monitoring and assistant solution for smart co-housing	Exploitation mechanism after ENACT	Follow-up projects on eHealth for cohousing
			Pilot deployment in ISRAA, with Italian translation of the Tellu Service
			Deployment of similar solutions to other welfare service providers

Category/ Market	eHealth, mHealth, welfare	Exploitation Plans (Explanation)	The partners will keep running and improving the pilot in ISRAA after the ENACT project, and introduce the results to ECHAlliance, a group of cohousing projects, and looking for further exploitation opportunities in other members of the alliance
Description of solution	The solution utilizes IoT devices deployed in the flat of the cohousing residents, to increase the interaction between residents and healthcare staff, saving cost and risks for physical contact	IP Protection	Open Source + Trial grant of Tellu Service to ISRAA
DevOps perspective	The development team and the co-housing providers need DevOps to continuously deliver tune the system, adding new devices, new features, improving the user experience, adjusting security policies etc.		
Trustworthiness perspective	The system needs to properly protect the residents' privacy, while being effective on monitoring and recording their health status, and their interaction with the healthcare staff.		

Table 14. Security a Remote patient monitoring and assistant solution for smart co-housing

2.2.3 Security and Privacy Risk Control over networks

Partners	Montimage, Beawre	Tools	T&S, RCA, Risk management
Name	Security and Privacy Risk Control over networks	Exploitation mechanism after ENACT	Commercialization: join commercialization strategy based on the combination of technologies provided by both companies. Consultancy services is also proposed to support customers
Category/ Market	Early adopters: **E-Health**: both security and privacy issues. IT companies (typically consultancy, integrators, or other big companies like Thales) in the e-health sector building IoT/Robotics for hospitals, health institutions Current Leads: TellU, Kampai. **Network operators**: we have a strong network in this field. Current Leads: Thales and Orange.	Exploitation Plans (Explanation)	Combining technology both from Montimage and Beawre to offer a joint solution. Montimage: interested in monitoring the ecosystem (e.g. robotics) in near real-time (technology based on their MMT monitoring framework). Beawre: to provide a higher layer for continuous risk control (reports, etc) to be compliant with GDPR, ISO 27001.

Description of solution	SaaS solution to prove strict compliance with continuous risk management requirements (ISO 27001, GDPR, etc). Our solution includes generation of automated reports, automated detection of security and privacy-related vulnerabilities, continuous monitoring of security and privacy risks, connected to multiple third-party tools in the DevOps cycle (i.e. Jira, Git, etc) and including online detection of vulnerabilities, attacks and changes, dashboards to understand the level of risk and support decision-making and prioritization and specific GDPR compliance dashboard. We also offer penetration testing on target system or simulated systems.	IP Protection	Core technology offered as open source with proprietary extensions for the commercial version. Part of the risk analysis technologies to be patented (AI techniques to improve risk management).
DevOps perspective	Our risk control approach is completely aligned with the DevOps principles. Our solution connects to tools in different phases of the DevOps cycle (Jira for planning, Git for coding, it can connect to testing and release and deployment tools and to the Montimage Monitoring Tool) to extract evidences and automatically calculate risk levels. In order to facilitate collaboration among the different stakeholders in the software development process, our solution provides a Kanban-like dashboard to allow for collaborative risk control.		
Trustworthiness perspective	By continuously monitoring risks related to security and privacy, our solution becomes essential to achieve early detection of potential issues and build more robust and trustworthy systems. In particular, one of the innovations in our tool is the provision of Knowledge bases to support engineers being compliant with legal obligations, thus feeling the existing gap between high level legal obligations imposed by regulations such as GDPR and the day-to-day practice by software engineers. In particular, our knowledge bases link Security and Privacy vulnerabilities, threats and mitigation actions. Our solution is also integrated with Mitre CWE open data.		

Table 15. Security and Privacy Risk Control over networks

3 Open challenges of interest for the community

Below are presented the main challenges of IoT DevOps that each of the ENACT technical outcomes is able to solve, and the remaining open challenges that we have identified that might be of interest to the community, in order to continue with the work carried out in ENACT once the project has ended. Additionally, we present for each tool how we envision its sustainability for the future.

Tool: Risk management
Main challenges solved during the project

During the execution of ENACT we have created a risk management methodology to control risks continuously. We have not only created the interfaces for agile risk management, but we have created generic mechanisms to control the effective implementation of mitigations actions and the monitoring of the effectiveness of these mitigation actions. Also, the knowledge base created during the project in collaboration with the H2020 PDP4E project, embedding open data from the CWE and CAPEC repositories, enables automated vulnerability detection. Besides, as an important outcome of this collaboration, we have integrated security and privacy aspects in the risk management process.

Open challenges of interest for the community

There remain many open challenges around the continuous control risks. First, risk management complexity grows with the increasing complexity of systems. AI approaches need to be studied in order to automate part of the risk management process and the activation of mitigation actions when risks severity go beyond certain thresholds. Besides, systems are not static. Systems change and business processes are executed that use these systems. An important research challenge is how to effectively control risks in real time over the execution of these business processes. Also, better coupling of risk management practices with financial information would allow for a better assessment of business impact and this is an important challenge to solve from a business perspective.

How it will be sustained after the end of the project

Beawre keeps a 5-years-time financial projection, which is updated monthly. This is very relevant information for investors and to guarantee the highest level of control of the sustainability of the company in the upcoming months and years. The technology generated in ENACT is at the core of our main technology and therefore, the sustainability of the results of this project are guaranteed as long as the company is sustainable. In particular Beawre has been very actively working to ensure the sustainability of the company:

- We have created an advisory board that has been actively working for the last 12 months to help us develop the business. This advisory board accumulate years of expertise in coaching start-ups, leveraging private investment and working and networking in the sectors targeted by Beawre.
- We have contacted and met more than 50 venture capital firms over the last 12 months.
- We have defined our first seed round ticket to be of around 500K € out of which 66% are already subscribed. We are looking for the final 160-180K € to close the round.
- Our team will grow in 10 new employees in the following 12 months after the investment round.
- Once we close the round, our main objectives are two:
    - **Customer acquisition**: We have the experience establishing conversations with high-level decision makers, but we lack experience in closing high-value contracts. We need to grow our sales pipeline to close more contracts. In order to solve this issue, we are planning to hire an experienced Head of Sales and, when necessary, sales representatives to increase sales pipeline performance. We are also planning to build up a support and services organization to ensure that development is not impacted.
    - **Extending technology**: In many cases, our clients need to increase the level of digitization of their processes before leveraging the potential of our tool. We also need to strengthen interoperability with other digital tools to increase market opportunities and ease user adoption. In general, B2B market implies strong legal requirements, and we need guidance to protect the company. Because of all these, we are planning to leverage the investment to create technology to help our customers to digitize their processes, to extend our current solution interoperability to connect to existing digital ecosystems, to hire technical staff to upscale technology development in response to demand, to obtain legal advice and to protect IP (e. g. through patents).
- Our estimations once the investment round is closed and thanks to the technology developed in ENACT is to increase the number of customers in the following 3 years to around **60** by the end of **2023**, assuming we hire a Head of Sales and a growing number of sales representatives (1 to 4) in the next 3 years.
- Besides, part of our core technology has been made public through a Research at Eclipse Initiative. We expect to continue working to engage the community and ensure the sustainability of the technology developed in the project through the engagement of engineers worldwide.

Tool: GeneSIS
Main challenges solved during the project
GeneSIS targets the challenge of supporting the automatic deployment of software, together with the attached security mechanisms, across the computing continuum from IoT, Edge to Cloud. Using GeneSIS, DevOps teams use a declarative modelling language to specify what software components and security mechanisms they want to deploy, and the engine automatically deploys them into the resources in the computing continuum, continuously monitoring the deployment status. The GeneSIS modelling language is independent of the underlying technologies, i.e., GeneSIS can deploy components anywhere in the IoT-Edge-Cloud continuum: from microcontrollers without direct Internet access to virtual machines running in the Cloud. It also includes security mechanisms as first-class modeling elements thus promoting security-by-design.
Open challenges of interest for the community
Among the open research challenges, we can mention the following three. First, availability strategies such as blue/green deployment cannot be applied on the smallest devices as it is often not possible to leverage virtualization or even to execute two instances of an application at the same time on such devices, novel strategies and patterns must be designed. Second, while we investigated support for security-by-design, and even if security contributes to privacy, specific support for privacy by design is still lacking in the literature. Last, solution for the context-aware and autonomous management of deployment is the next step toward facilitating DevOps teams in operating SIS. The models@run.time pattern adopted by GeneSIS provides strong baseline for this.
How it will be sustained after the end of the project
GeneSIS will be further developed in our subsequent research project (i.e., the FLEET Norwegian project). It is envisioned to further extend the monitoring abilities offered by GeneSIS (more runtime data, including inferred data, being added into the GeneSIS runtime model), which when integrated with DivEnact will further improve the fleet deployment strategies.

Tool: ACM: Actuation Conflict Management
Main challenges solved during the project
The main challenge solved by the Actuation Conflict Management Enabler was to enable the identification and the resolution of direct and indirect actuation conflicts on large scale and highly distributed Smart IoT Systems (SIS). As this challenge was part of a DevOps development cycle, we opted for a pattern-based approach to identifying and resolving conflicts, emphasising reusability, yet maintaining high-quality level. Thus, on the basis of a structural model of the SIS, issued from the GeneSIS deployment tool and complemented by SIS designers with information on actuator physical effects, pre-defined direct and indirect conflict patterns are locally identified. Then, off-the-shelf actuation conflict managers are proposed to designers for their resolution, advocating reusability and significantly reducing the development cycle time. Would off-the-shelf managers be irrelevant, a complete flow is proposed to design custom managers with an original approach by successive refinement and validation from specification to implementation. The first step allows to specify the logical behaviour of the actuation conflict handlers and to formally validate their properties by model checking. The second step aims at simulating different implementation strategies of the actuation conflict managers immersed in different asynchronous environments, relying on the DEVS formalism and characterising the timings of the heterogeneous hardware platforms on which they are likely to be deployed at the edge of the infrastructure. The last step generates the code for the actuation conflict handlers according to the intended target. The refinement approach minimises the errors that can be injected by the designers while allowing them to intervene finely in the design of the custom ACM.
Open challenges of interest for the community
SIS designers are required to describe the physical effects of the actuators involved in the system. As this task can be time-consuming and error-prone, it would be worth taking advantage of web semantic tools to automate this step. However, the main challenge here lies in managing the semantic heterogeneity of the descriptions of the actuators leveraged by the SIS at the edge of the infrastructure
How it will be sustained after the end of the project

The concepts underlying the Actuation Conflict Manager Enabler are currently discussed with the Technology Transfer Accelerator Office (SATT). In collaboration with the university, the role of this office is to accelerate the process of technology transfer from publicly funded research towards the industry.

Tool: TaS: Test and Simulation

Main challenges solved during the project

The main challenge solved by the Test and Simulation Enabler was the difficulty of testing IoT application/system. When it comes to build a testing environment for testing IoT application/system, there are many problems that need to be covered such as: unstable network connection, short life battery, low energy level, and especially the stable of the surrounding environment. To eliminate those problems, the Test and Simulation enabler provides a flexible simulation model which allow to test IoT application/system in many different scenarios, such as: abnormal sensor behaviours, cyber security attack, and scalability. It also supports automation testing and easy integration within any DevOps cycle. The tool also supports recording the data from a real system and its use as testing dataset that can be modified.

Open challenges of interest for the community

Inspired by the concept of Digital Twins, the Test and Simulation enabler is still missing a more predictive process that needs to be completed. By implementing Machine Learning based on the recorded and simulated datasets, the tool can simulate and provide some predictions based on specific input data. This will bring great value for decision making process.

How it will be sustained after the end of the project

The Test and Simulation enabler is going to be extended to be part of the intelligent security monitoring and enforcement framework in the H2020 project PRECINCT.

Tool: OLE: Online Learning Enabler

Main challenges solved during the project

The main challenge solved by the Online Learning Enabler (OLE) was to enable a smart IoT system (SIS) to adapt themselves to a continuously changing context by leveraging machine learning techniques. To solve this challenge we mainly employed a modern variant of Reinforcement Learning (policy-based) to make the SIS choose adequate adaptation actions based on their perception of their environments and system states. By leveraging policy-based RL we were able to overcome the need for manual quantization of the state space and could also deal with continuous adaptation variables (such as system parameters). As an additional feature of OLE, we proposed algorithms to optimize the exploration phase of RL algorithms in the presence of large, discrete adaptation spaces by leveraging the structure of the system's feature model. Finally, we employed the concept of reward decomposition, we provided insights into the decision making process of value-based RL (i.e., towards explainable AI).

Open challenges of interest for the community

Applying RL in a pure only fashion may lead to poor initial performance of the SIS due to the trial-and-error nature of RL leading to a rather long exploration phase. We showed that this exploration phase can be significantly shortened by pretraining the applied policy before it is used online (e.g. with the help of a simulation). However, there is still room for improvement, especially when an RL approach should be able to initially perform better in a range of different online situations. One option for further improvement might be the application of Meta RL methods.

How it will be sustained after the end of the project

The concepts and prototypes underlying the OLE tool are currently serving as basis for further development in the H2020 project DataPorts. Where, in particular, policy-based RL is leveraged to facilitate the proactive adaptation of data-driven business processes.

Tool: BDA: Behavioural Drift Analysis

Main challenges solved during the project

The main challenge solved by the Behavioural Drift Analysis Enabler was first to enable Smart IoT Systems (SIS) to be assessed for effectiveness at run-time, yet embracing the complexity of the physical environment beyond the SIS itself.

To meet this challenge, we borrowed from the theory of complex systems and adopted a systemic approach that considers the purposes of SIS rather than their means. Therefore, unlike state-of-the-art test and verification techniques usually involved at design time that builds on analytical models, the proposed method relies on stochastic models of the legitimate effects SIS have to produce in the physical environment, irrespective of their implementation.

The second challenge was to provide SIS designers with a tool to analyse SIS ineffectiveness by providing clear information on their symptoms. To meet this challenge, a novel algorithm has been developed that first learns SIS concrete behaviour from field observations and, whenever applicable, generates a dissimilarity graph that makes clear the structural and parametric differences (i.e., the symptoms) with the model of the legitimate effects SIS have to produce in the physical environment

Open challenges of interest for the community

Stochastic models of the legitimate effects SIS have to produce in the physical environment are complex to develop from scratch; this process involves counterparts knowledgeable on the SIS and their operational environment. The model learning algorithm developed as part of this enabler may provide a first draft.

How it will be sustained after the end of the project

The concepts underlying the Behavioural Drift Analysis Enabler are currently serving as a basis for further developments in a partnership chair of the foundation of the University Côte d'Azur called "UX for SMART LIFE: Home & Mobility". SIS effectiveness assessment is then translated into Users' satisfaction assessment for Smart UX Design.

Tool: RCA: Root Cause Analysis

Main challenges solved during the project

In complex systems, determining the causal factors of observed anomalies can be drastically difficult and time consuming due to the exceeding amount of data sources (e.g., logs, traffic, metrics) needed for identifying the status of the system. Root Cause Analysis's (RCA) objective is to infer the root-causes of problems by analysing the causal chains governing the system being monitored. RCA plays a vital role in the Risk Management process which principally includes vulnerability scanning, anomaly detection, root-cause analysis, and remediation. The tool is applicable to all systems where collecting monitoring data is possible. In principle, it consists of the construction of a historical database of known/learned incidents, together with their corresponding symptoms, root-causes, impacts and mitigation actions based on the experts' experience, as well as the calculation of the similarity between the symptoms of new incidents with the ones stored in that database.

Open challenges of interest for the community

As a Machine Learning-based solution, the efficiency of the tool depends remarkably on the quality of the learning datasets. It requires enough relevant monitoring data attributes and significant domain/system knowledge for obtaining good results from the analysis. Open challenges are on the data collection, the feature selection, as well as on the response time when the historical database of learned events becomes more voluminous and sophisticated.

How it will be sustained after the end of the project

The tool will be extended and adapted in several other European projects dealing with different contexts, namely INSPIRE-5GPLUS and SANCUS (5G Mobile networks), VeriDevOps (security, big data, AI/ML) and PRECINCT (4G/5G/IoT) as well as to become an important tool in the ecosystem of Montimage to be commercialized together within the MMT-Box (https://montimage.com/products/MMT_Box.html)

Tool: Security and Privacy Monitoring Enabler

Main challenges solved during the project

The main challenges solved by the tool relate to the major features and innovation it brings:

- Ensuring holistic security assurance for IoT systems at operation, particularly small companies that cannot afford expensive SIEM solutions have strong needs to guarantee high security levels and data protection at all times.
- Scalable and continuous Security monitoring of IIoT with multi-layer holistic information and advanced situational awareness.
- Advance anomaly detection based on behaviour profiling and not only signature-based detection.
- Monitoring of communication security and network status for those IoT systems that use industrial protocols such as Modbus, DNP3, MQTT, etc.
- Easy to understand overview of different issues identified at network, application and device layer, in a single dashboard.
- Compliance with GDPR starts from strong protection of personal data, therefore, ensuring cybersecurity is core to privacy protection.

Open challenges of interest for the community

In order to ensure security at SIS operation, the difficulties to monitor distributed IIoT environments add up to the lack of automatic remediation in case of security requirements violation at runtime. The particularities of technologies and solutions used in each IIoT system make security automation difficult. In ENACT this was solved for secure communications through SMOOL middleware (see below). The security orchestration and automation, as well as the interoperation of healing mechanisms are still open challenges.

How it will be sustained after the end of the project

The asset will be commercialised among Tecnalia clients by Tecnalia ICT Division with the support of Tecnalia Ventures. The challenge in the commercialisation is the industrialisation of the proof-of-concept towards a more mature product, for which internal investments would be necessary.

Tool: Security-aware SMOOL IoT Platform (Control Enabler)

Main challenges solved during the project

The main challenges solved by the security enhancements to SMOOL ontology and the tool can be summarised as follows:

- Grant interoperability and secure communications between things-edge in those IoT environments where the ontology-based IoT middleware SMOOL is deployed.
- IoT application security monitoring and enforcement by enforcing confidentiality, integrity and availability of things-edge communication.
- Integration of secure IoT platforms with MDE approaches for security-by-design to ease the design, configuration and deployment of security mechanisms ready to directly use them at runtime.

Open challenges of interest for the community

Interoperability of IoT platforms among them and how to enlarge security ontologies with privacy ontologies in IoT middleware.

How it will be sustained after the end of the project

The SMOOL project is an open source project which will be enlarged and enriched by the Community and it will be followed up by Tecnalia in future research projects.

Tool: CAAC: Context-Aware Access Control

Main challenges solved during the project

The main challenges solved by the Context-Aware Access Control (CAAC) were to provide one unique tool to control in the same way the access of all the IoT actors (end-users, services, devices, administrators) to the operated data and resources, for both IT and OT (operational technologies) domains, and to allow

context-aware dynamic access control behaviors by adapting the provided authorizations based on a risk level computed from contextual data on the user and his devices. Solving this challenge required adding dynamicity to the authorization decisions the OAuth 2.0 standard protocol produces to make the provided authorizations responsive to the context, by injecting contextual risk levels as dynamic scopes in the standard Device flow.

Open challenges of interest for the community

Modeling the contextual risk that should be considered in identity and access management solutions remains an open question, especially when these solutions are applied to the IoT use cases, where context of devices and users is continuously changing. We will keep investigating this open question as part of our research for the development of our future offer "Evidian Prescriptive IAM".
How it will be sustained after the end of the project
Evidian Web Access Manager (WAM) provides security features for identity management and access control based on the OAuth2 and OpenID Connect (OIDC) protocols. The Context-Aware Access Control tool is an evolution of the authentication and authorization mechanisms provided by WAM intended for the Internet of Things. It will be integrated in the Evidian standard offer as a key component of the new “Prescriptive IAM” offer. Evidian will first target the sector of HealthCare, considering the success that resulted from the Digital Health use case in ENACT. Then other Evidian customers will be addressed, as well as new prospects in each domain addressed by Evidian: Manufacturing/Retail/Transports, Public Health, Finance/Services and Telecom/Media/Utilities. The context-aware capacity of the tool will be leveraged in this future “Evidian Prescriptive IAM” solution. In this objective, further investigations on risk models and AI-augmented techniques applied to identity and access management will be carried out, in order to develop a prescriptive enforcement of authentication and authorization decisions, based on risk indicators.

Tool: DivEnact: Diversity-oriented fleet deployment
Main challenges solved during the project
DivEnact targets at a fundamental challenge towards automatic deployment of software in smart IoT systems, i.e., how to allow developers to deploy software into the fleet of devices as whole, instead of handling each device individually. We have initial progress to solve this challenge by utilizing model-driving engineering and constraint solving. We also investigated the typical DevOps operations required by developers when deploying software into a fleet of devices, and provide support to these operations through a graphical user interface.
Open challenges of interest for the community
Fleet deployment is still an open question, in terms of how to assign software variants into the proper devices consider their context. We need to further understand the requirements from DevOps teams, which is often specific to vertical domains. It is also important to assign software variants to achieve better performance, which is not touch yet in this project. We will keep investigating the concept and these open questions in our subsequent projects.

4 Conclusion: Sustainability of the project

This deliverable summarizes the planned activities after the project ends, to exploit the project results and achieve the sustainability of the project work.

Our main focus is to promote the ENACT enablers to the potential users, i.e., the DevOps teams for Smart IoT systems. For this purpose, four different routes have been identified, which define the Roadmap of the project in terms of commercialization, knowledge and technology transfer, community building and engagement, and domain activities deploying the ENACT tools and solutions developed. These four routes group the different exploitation plans and activities envisioned by the partners of the consortium establishing the paths and directions that are and will be followed once the project has ended. Joint exploitation plans have also been defined by all the ENACT partners, showing how partners will continue collaborating after ENACT, and how the different tools will continue evolving together to continue pushing the DevOps technologies of ENACT forward.

For different partners, these post-project activities will be conducted alongside the marketing plans, the subsequent research and innovation projects, or a mix of them. The table below summarizes the granted research and innovation projects as of March 2021, where ENACT results will be further developed and exploited.

Partner	Project Name	Program	Time	ENACT results	Comment
Tellu, SINTEF	FLEET: Fleet-Oriented Intelligent Operation of Large Scale Edge System	Innovation Project for the Industrial Sector 2019	2020-2024	GeneSIS, DivEnact	We will apply the fleet deployment toolset to the production of Tellu, and another Norwegian SME, Dolittle AS
SINTEF, Tellu	ERASTOSTHENES: Secure management of IoT devices lifecycle through identities, trust and distributed ledgers	H2020-SU-DS-2020 (RIA)	2021-2025	GeneSIS, DivEnact	We will investigate the use of fleet deployment theory and tools for the trustworthy deployment of novel secure management components in IoT
MI	INSPIRE-5Gplus: INtelligent Security and Pervaslve tRust for 5G and Beyond	H2020-ICT-2018-2020 (RIA)	2019-2022	RCA	Our generic RCA tool that has been evaluated in IoT systems in the context of ENACT will be extended/ adapted to 5G environment. Root Cause Analysis techniques will be devised to identify the cause and determine the responsibility when security breaches occur inside a 5G virtualized infrastructure or between parties.
MI	SANCUS: analysis software scheme of uniform statistical sampling, audit and defence processes	H2020-SU-ICT-2018-2020 (RIA)	2020-2023	RCA	Root Cause analysis to understand the origin of the detected security incidents by combining probabilistic decision trees refined by AI/ML defence strategies, which will help to improve the capacity of the system in forecasting potential threats related to Docker components.
MI	VeriDevOps: Automated Protection and Prevention to Meet Security Requirements in DevOps Environments	H2020-ICT-2018-20 (RIA)	2020-2023	RCA	We will develop an automated Root cause analysis engine (RCA) for DevOps and QA Engineers by incorporating big data and machine learning to quickly identify security issues and their causes. This engine relies on a systematic process for identifying “root causes” of problems or events and an approach for responding to them.
MI	PRECINCT: Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyberphysical Threats and effects with focus on district or regional protection	H2020-SU-INFRA-2018-2019-2020 (IA)	2021-2023	RCA & TaS	RCA and TaS will be extended to be a part of the intelligent security monitoring and enforcement framework for 4G/5G/IoT networks in Critical Infrastructures (e.g.; smart cities, energy, transport, telecommunications)

UDE	DataPorts: A Data Platform for the Connection of Cognitive Ports	H2020-Big-Data-Value-PPP	2021-2023	OLE	The concepts and prototypes underlying the OLE tool are currently serving as basis for further development in the H2020 project DataPorts. Where, in particular, policy-based RL is leveraged to facilitate the proactive adaptation of data-driven business processes.

As part of the community building effort, and potentially with the help of OW2, SINTEF will call for 2 ENACT gathering events within 5 years after the project ends, inviting ENACT partners to meet and discuss the new development of the tools, and exchange the exploitation progresses and opportunities. New and potential users of the ENACT tools will also be invited. The meetings will be co-located with large European events, such as IoT Week, or EC's ICT Event.

The impact and the sustainability of the ENACT project also goes beyond the direct exploitation of its results. As a Research and Innovation Action, the goal of the ENACT project was to enable DevOps in the realm of trustworthy smart IoT systems. We identified different challenges for this new topic, and during the lifespan of the project, we conducted thorough research to meet these challenges, through the technologies and tools developed. This document collects these main challenges that were successfully addressed, and the remaining open challenges of interest to the community, as well as the planned paths. In addition to the subsequent dissemination of the research activities and the results through academic and industrial venues, ENACT partners will take advantage of our membership in various organizations to convey the knowledge we developed on smart IoT systems into the white papers, research strategies, long-term plans, etc. In particular, we will focus on the following organizations:

- **NESSI** (The European Technology Platform dedicated to software services and data). INDRA, SINTEF and UDE are in the NESSI board, and UDE is the vice chair of the NESSI steering committee. Our objective in NESSI is to promote the importance of software engineering methods (in particular DevOps) and environments for the Key Digital Technologies (KDT), including IoT and Edge. SINTEF and UDE co-authored the NESSI position paper in this topic[4], envisaging the role of software engineering in KDT and the main challenges. We will follow up the topic based on the position paper.
- **AIOTI** (The alliance for the Internet of Things Innovation). SINTEF and Tecnalia are active members of AIOTI.
- **BDVA** (Big Data value association): (Big Data value association): INDRA, SINTEF, Tecnalia, and UDE are Full Members of the Association, and UDE is deputy secretary general. Our objective in BDVA is to promote the importance of software engineering methods (in particular DevOps) and environments for data-intensive and AI-based systems, which includes the role data-driven AI plays for building future software engineering tools and techniques, but also how to build AI-based systems (including constructive and analytics quality assurance).
- **NetworldEurope**. Montimage is a board member of NetworldEurope and 5GPPP working groups.
- **ECHAlliance** (European Connected Health Alliance). ISRAA has launched a Treviso Ecosystem in the perimeter of the world-wide network run by ECHAlliance[5]. The topics that are in the core of the Ecosystema are the digital transformation in the care of the elderly, trying to foster the implementation EU wide of the main solutions currently available through the use of mobile devices, robots and the connection between these and IoT devices and various forms of artificial intelligence.

[4] http://www.nessi-europe.com/default.aspx?Page=position%20papers
[5] https://echalliance.com/report-of-the-launch-event-of-the-treviso-health-social-care-ecosystem/

Appendix A. Beawre's awards media impact

The different awards received by Beawre Digital have generated a very strong presence for Beawre in digital media worldwide, specially related to wining the CEMEX Ventures Startup Competition and being selected as part of the CEMEX Top50 list of most promising startups in the sector, worldwide. As an example, you can see a sample of some of the press releases published by some of the most relevant actors in the sector and significant industrial communities:

- Beawre Digital | CEMEX Ventures: https://www.cemexventures.com/projects/beawre-digital/
- Construction Startup Competition 2020 : meet the winners! | Leonard, foresight and Innovation by VINCI: https://leonard.vinci.com/en/construction-startup-competition-2020-meet-the-winners/
- Cemex Ventures announces 10 finalists in construction tech startup competition | Construction Dive: https://www.constructiondive.com/news/cemex-ventures-announces-10-finalists-in-construction-tech-startup-competit/591473/
- CEMEX Ventures launch the 50 most promising startups in the 2020 construction ecosystem and the cities of the future - CEMEX Ventures launch the 50 most promising startups in the 2020 construction ecosystem and the cities of the future - CEMEX: https://www.cemex.com/-/cemex-ventures-launch-the-50-most-promising-startups-in-the-2020-construction-ecosystem-and-the-cities-of-the-future
- CEMEX Ventures names Construction Startup Finalists | Technology & AI | Construction Global: https://www.constructionglobal.com/technology-and-ai-1/cemex-ventures-names-construction-startup-finalists
- Cemex Ventures anuncia a 10 finalistas en la competencia de startups de tecnología de la construcción – Portal CDT (registrocdt.cl): https://www.registrocdt.cl/cemex-ventures-anuncia-a-10-finalistas-en-la-competencia-de-startups-de-tecnologia-de-la-construccion/
- Construction Startup Competition Yield Global Top 50 Contech startups (builtworlds.com): https://builtworlds.com/news/2020-review-major-construction-startup-competition-brings-global-top-50-contech-startups/
- Anuncian finalistas de competencia de startups de tecnología de la construcción promovida por Cemex Ventures – Productos y soluciones (costosperu.com): http://www.productos-y-soluciones.costosperu.com/id/anuncian-finalistas-de-competencia-de-startups-de-tecnologia-de-la-construccion-promovida-por-cemex-ventures/
- Cemex Ventures anuncia a 10 finalistas en la competencia de startups de tecnología de la construcción | Prensa Real Estate: http://prensarealestate.com/cemex-ventures-anuncia-a-10-finalistas-en-la-competencia-de-startups-de-tecnologia-de-la-construccion/
- Meet the Winners of the 'Construction Startup Competition 2020' Ferrovial: https://newsroom.ferrovial.com/en/news/meet-the-winners-of-the-construction-startup-competition-2020/
- Cemex Ventures announces 10 finalists in construction tech startup competition - You Startups: https://youstartups.com/cemex-ventures-announces-10-finalists-in-construction-tech-startup-competition/
- UK Construction Week - Cemex Ventures announces 10 finalists in construction tech startup competition (constructionbuzz.co.uk): https://news.constructionbuzz.co.uk/en/article/93738/cemex-ventures-announces-10-finalists-in
- DEAL - Magazine | Real Estate | Investment | Finance (deal-magazin.com): http://www.deal-magazin.com/news/96812/Construction-Startup-Competition-Bauplaner-Construyo-setzt-sich-durch
- Meet the winners of 2020 Construction Startup Competition | NOVA by Saint-Gobain (nova-saint-gobain.com): https://www.nova-saint-gobain.com/en/newsroom/meet-winners-2020-construction-startup-competition
- Communiqué de presse - 14 décembre 2020 | CEMEX France: https://www.cemex.fr/-/communique-de-presse-14-decembre-2020

• 6. Adoption of (new) technologies | Center for Integrated Facility Engineering (stanford.edu): https://cife.stanford.edu/aec-and-pandemic-december-2020-sub-6
• Cemex Ventures оголошує 10 фіналістів конкурсу стартапів у сфері будівельних технологій - BUDUEMO.COM - професійний будівельний портал: https://buduemo.com/ua/news/word_news/cemex-ventures-objavljaet-10-finalistov-konkursa-startapov-v-sfere-stroitelnyh-tehnologij.html